Information Technology Services

Information and Cybersecurity Awareness

Email ithelp@up.ac.za | **www.up.ac.za/itsecurity**

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

CyberUP
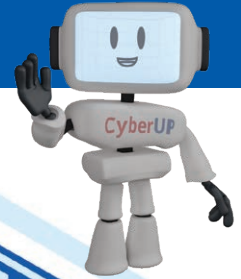
Managing your personal IoT network
'Make your home a haven for online safety'

Billions of technological devices are constantly communicating across the internet. Many of these are in private homes and include things such as personal assistants, smart watches, security cameras, TVs and vacuum cleaners. Have you ever considered the possibility that they could be a risk to your personal safety?

Introduction

The Internet of Things, or IoT, consists of connected devices that have unique identifiers and transfer data over a network without requiring human-to-human or human-to-computer interaction—although people can interact with them to set them up, give them instructions or access their data.

These smart devices collect, send and act on data that they acquire from their environments. The collected data may be shared with other devices or sent to the cloud to be analysed.

Many home users do not consider these devices when they think about the security of their home networks, or simply assume that their newly purchased devices are secure enough.

However, security standards for IoT technology are still being developed and are not yet universally accepted or enforced and manufacturers, most of whom are trying to provide new functionalities faster than their competitors, may not give security aspects the necessary attention.

The risk involved when criminals obtain access to an IoT device is that sensitive and personal information and images could be stolen, or that the compromised device could be used as a gateway to other devices in the network.

Securing your IoT devices

Securing your IoT devices might seem like a daunting task. However, the following tips can help you to do so:
- Make sure your wireless router is configured to be secure.
- On many devices, default passwords for the administrator's account are searchable on the internet. Therefore, you should change the pre-set password on all of your devices.
- Check factory default settings on the device and harden them to provide increased security.
- Enable updates to the firmware of the device.
- Switch off devices when not in use.
- Maintain separate networks for your user devices (computers, cellphones, etc) and other IoT devices.

SEE MORE

▶ WATCH: A hacker discusses IoT security

READ MORE

📖 Everything you need to know about the IoT
My new air fryer is a security risk

DO MORE

Try to find the default passwords for your router and other IoT devices on the internet
Create a separate network for your smart home devices